09/622371

Sheet 1 of 4

FORM PTO-1449 (REV. 7-80)	U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. ASA-907	SERIAL NO.
		APPLICANT K. MIYAZAKI et al	
		FILING DATE August 16, 2000	GROUP

LIST OF DOCUMENTS CITED BY APPLICANT

(Use several sheets if necessary)

U.S. PATENT DOCUMENTS

* EXAMINER INITIAL		DOCUMENT	DATE	NAME	CLASS	SUBCLASS	FILING DATE *(If Appropriate)*
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

FOREIGN PATENT DOCUMENTS

		DOCUMENT	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION	
							YES	NO
	AL						□	□
	AM						□	□
	AN						□	□
	AO						□	□
	AP						□	□

OTHER DOCUMENTS *(Including Author, Title, Date, Pertinent Pages, etc.)*

mpn	AR		SMART CARD HANDBOOK, John Wiley & Sons, 1997, R. Effing.
	AS		BANKING- SECURE CRYPTOGRAPHIC DEVICES (RETAIL) - Part 1: Concepts, Requirements and evaluation methods, First Edition, June 15, 1998, ISO13491, ISO13491-1.
	AT		DPA, Introduction to Differential Power Analysis and Related Attacks, 1998, P. Kocher et al.

EXAMINER Nguyen	DATE CONSIDERED 2/23/04

* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

09/622371

Sheet 2 of 4

FORM PTO-1449 (REV. 7-80)	U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. ASA-907	SERIAL NO.
LIST OF DOCUMENTS CITED BY APPLICANT *(Use several sheets if necessary)*		APPLICANT K. MIYAZAKI et al	
		FILING DATE August 16, 2000	GROUP

U.S. PATENT DOCUMENTS

* EXAMINER INITIAL		DOCUMENT	DATE	NAME	CLASS	SUBCLASS	FILING DATE *(If Appropriate)*
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

FOREIGN PATENT DOCUMENTS

		DOCUMENT	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION	
							YES	NO
	AL						□	□
	AM						□	□
	AN						□	□
	AO						□	□
	AP						□	□

OTHER DOCUMENTS *(Including Author, Title, Date, Pertinent Pages, etc.)*

MDN	AR	Timing Attacks on Implementations of Diffie - Hellman, RSA, DSS, and Other Systems, CRYPTO'96, 1996, P. Kocher.
↓	AS	Working Draft: AMERICAN NATIONAL STANDARD X.9.63-199x Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography, American National Standards Institute, January 9, 1999.
↓	AT	Standard Specifications for Public Key Cryptography (Draft Version 9), IEEE P1363 Standard, IEEE, February 8, 1999.

EXAMINER	DATE CONSIDERED 2/23/04

* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

09/622371

Sheet 3 of 4

FORM PTO-1449 (REV. 7-80)	U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. ASA-907	SERIAL NO.
LIST OF DOCUMENTS CITED BY APPLICANT *(Use several sheets if necessary)*		APPLICANT K. MIYAZAKI et al	
		FILING DATE August 16, 2000	GROUP

U.S. PATENT DOCUMENTS

* EXAMINER INITIAL		DOCUMENT	DATE	NAME	CLASS	SUBCLASS	FILING DATE *(If Appropriate)*
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

FOREIGN PATENT DOCUMENTS

		DOCUMENT	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION	
							YES	NO
	AL						□	□
	AM						□	□
	AN						□	□
	AO						□	□
	AP						□	□

OTHER DOCUMENTS *(Including Author, Title, Date, Pertinent Pages, etc.)*

MON	AR		Speeding up the computations on an elliptic curve using addition-subtraction chains, Theoretical Informatics and Applications, Vol. 24, No. 6, 1990,
			F. Morain et al.
	AS		APPLIED CRYPTOGRAPHY, John Wiley & Sons, Inc., 1996, B. Schneier, pp. 466-469.
	AT		HOW TO SHARE A SECRET, COMMUNICATIONS OF THE ACM, Vol. 22, No. 11, 1979, A. Shamir, pp. 612-613.

EXAMINER	DATE CONSIDERED 2/23/04

09/622371

533 [illegible]'d PCT/PTO 16 AUG 2000

Sheet 4 of 4

FORM PTO-1449 (REV. 7-80)	U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. ASA-907	SERIAL NO.
LIST OF DOCUMENTS CITED BY APPLICANT *(Use several sheets if necessary)*		APPLICANT K. MIYAZAKI et al	
		FILING DATE August 16, 2000	GROUP

U.S. PATENT DOCUMENTS

* EXAMINER INITIAL		DOCUMENT	DATE	NAME	CLASS	SUBCLASS	FILING DATE *(If Appropriate)*
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

FOREIGN PATENT DOCUMENTS

		DOCUMENT	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION	
							YES	NO
	AL						□	□
	AM						□	□
	AN						□	□
	AO						□	□
	AP						□	□

OTHER DOCUMENTS *(Including Author, Title, Date, Pertinent Pages, etc.)*

MPN	AR		Working Draft AMERICAN NATIONAL STANDARD, X9.62 - 1998, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), American National Standards Institute, September 20, 1998.
	AS		
	AT		

EXAMINER	DATE CONSIDERED 2/23/04

Sheet 1 of 1 #7

FORM PTO-1449 (REV. 7-80)	U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. ASA-907	SERIAL NO. 09/622,371
LIST OF DOCUMENTS CITED BY APPLICANT *(Use several sheets if necessary)*		APPLICANT K. MIYAZAKI et al	
		FILING DATE 8/16/00	GROUP

U.S. PATENT DOCUMENTS

* EXAMINER INITIAL		DOCUMENT	DATE	NAME	CLASS	SUBCLASS	FILING DATE *(If Appropriate)*
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

FOREIGN PATENT DOCUMENTS

		DOCUMENT	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION YES	TRANSLATION NO
mon	AL	10282881	10/23/98	Japan			☒	□
↓	AM	3-76447	4/2/91	Japan			☒	□
	AN	11316542	11/16/99	Japan			☒	□
	AO						□	□
	AP						□	□

OTHER DOCUMENTS *(Including Author, Title, Date, Pertinent Pages, etc.)*

mon	AR	B. Schneider, "Applied Cryptography (Second Edition)," John Wiley & Sons, Inc. (1996), pp. 71-73.
↓	AS	K. Takaragi, et al, "Current Cards Society and Security Technology," The Japanese Society of Printing Science and Technology, Vol. 29, No. 3 (113rd volume), pp. 288-295.
	AT	Yuichi Kaji, et al, "Personal Authentication by Password declare-next authentication-Secure Personal Authentication by Magnetic Card Technical Report of the Institute of Electronics, Information and Communication Engineers (ISEC 95-39 to 44) Vol. 95, No. 423, pp. 21-28.

EXAMINER	DATE CONSIDERED 2/23/04

* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.